



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,672	06/04/2001	Prakash Panjwani	06944.0036	2391
293	7590	03/08/2006	EXAMINER	
Ralph A. Dowell of DOWELL & DOWELL P.C. 2111 Eisenhower Ave Suite 406 Alexandria, VA 22314			NGUYEN, MINH DIEU T	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/871,672

Applicant(s)

PANJWANI ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-48 is/are pending in the application.
- 4a) Of the above claim(s) 1-6 is/are withdrawn from consideration.
- 5) ☒ Claim(s) 7-26 and 48 is/are allowed.
- 6) ☒ Claim(s) 27-35 and 37-46 is/are rejected.
- 7) ☒ Claim(s) 36 and 47 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated December 14, 2005 with the amendment to claims 27 and 38.
2. Claims 7-48 are pending.

Response to Arguments

3. Applicant's arguments, filed December 14, 2005 have been fully considered. The rejection of claims 7-26 and 48 has been withdrawn.
4. Applicant states in the remark (page 9), Blake-Wilson does not teach generating a pair of secret keys, the examiner clearly agrees on it. However, applicant agrees Blake-Wilson at most teaches generating a MAC using a single shared secret key and this is relied on for the teaching of "base station computing a shared secret to be shared with the mobile station" in claims 27 and 38.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 27 and 38** are rejected under 35 U.S.C. 102(e) as being anticipated by Blake-Wilson et al. (6,336,188) with Diffie-Hellman (New Directions in Cryptography) incorporated herein by reference (see Blake-Wilson, col. 2, lines 42-46).

Blake-Wilson discloses a key agreement method between a pair of entities i and j (col. 1, lines 62-63, i.e. base station and mobile station, correspondingly), each correspondent has a respective identity (col. 2, line 19), the first correspondent having a private key and a public key derived therefrom (col.1, lines 63-64), the method comprising of each participant generates a public/private key pair, wherein the public key along with user's name are made public, while the private key must be kept secret (see Diffie-Hellman, incorporated by reference from Blake-Wilson, page 644, right column, second paragraph; page 648, left column, fifth paragraph). It anticipates base station accesses secret public key of the mobile station.

Blake-Wilson discloses entity i computing a shared secret key k' using entity j's public key and i's private key (col. 2, lines 13-15), entity i using shared secret key k' to compute an authenticated message on entity identities i, j and entities public session keys and forward the authenticated message to entity j (col. 2, lines 16-20).

Blake-Wilson discloses the random challenge element in computing the authenticated message (col. 3, lines 19-52) anticipates random challenge parameter (i.e. short-lived public key) in computing MAC for use in authenticating the stations to one another.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. **Claims 28-29 and 39-40** are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake-Wilson et al. (6,336,188) in view of Reeds, III et al. (5,153,919).

a) **As to claims 28 and 39**, Reeds discloses the service provider could supply each mobile with its own pair of private and public keys (col. 2, lines 30-31), the second correspondent obtains the public key from a service provider of the first correspondent (col. 3, lines 8-23; col. 8, lines 5-6).

b) **As to claims 29 and 40**, Reeds discloses the second correspondent is a service provider of the first correspondent (Fig. 1).

9. **Claims 30-31 and 41-42** are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake-Wilson et al. (6,336,188) in view of Reeds, III et al. (5,153,919) and further in view of Diffie et al. (Re. 36,946).

Blake-Wilson and Reeds do not disclose the service provider obtaining the public key by a manual exchange at a distributor outlet.

Art Unit: 2137

Diffie discloses the public key is transmitted to the service provider by a manual exchange using a dial-up connection (col. 5, lines 61-63). Diffie does not disclose dial-up connection, however it is quite known in data communications art. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dial-up connection so as to provide variety of means to exchange public key.

10. **Claims 32-33 and 43-44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake-Wilson et al. (6,336,188) in view of Reeds, III et al. (5,153,919), further in view of Maruyama et al. (5,883,960).

Reeds discloses the ESN number is installed in the mobile unit by the manufacturer at the time the unit is built, however Blake-Wilson and Reeds do not disclose the service provider obtains the public key by an exchange at manufacture time.

Maruyama discloses the mobile unit public keys are written during the manufacture of the mobile units (col. 9, lines 15-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use exchanging public key at manufacture time in the system of Blake-Wilson and Reeds as Maruyama teaches so as to provide variety of means to exchange public key.

11. **Claims 34-35 and 45-46** are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake-Wilson et al. (6,336,188) in view of Reeds, III et al. (5,153,919) and further in view of Quick, Jr. (6,260,147).

Blake-Wilson and Reeds do not disclose service provider obtains public key by an over-the air exchange and the exchange is secured using a password.

Quick discloses the service provider obtains public key by an over-the air exchange and the exchange is secured using a password (Fig. 1; col. 2, lines 30-47).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use exchanging public key over the air exchange in the system of Blake-Wilson and Reeds as Quick teaches so as to provide variety of means to exchange public key.

12. **Claim 37** is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake-Wilson et al. (6,336,188) in view of Venkatesan et al. (6,209,093).

Blake-Wilson do not disclose using elliptic curve to compute the private keys, public keys and MACs.

Venkatesan discloses the private, public keys and MACs are computed using elliptic curve cryptography (col. 10, lines 33-53).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of elliptic curve cryptography to compute public, private keys and MACs in the system of Blake-Wilson as Venkatesan teaches so as to make the system more efficient.

Allowable Subject Matter

13. Claims 36 and 47 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

14. Claims 7-26 and 48 are allowed.

Claims 7 and 48: the prior arts of record do not teach first correspondent combining its private key with the short-lived public key and generating a pair of secret keys.

Claims 8-26 are allowed because of dependency.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

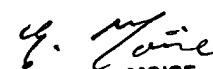
Art Unit: 2137

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


mdn
3/3/06


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER